



Technical briefing on

Multifactor authentication

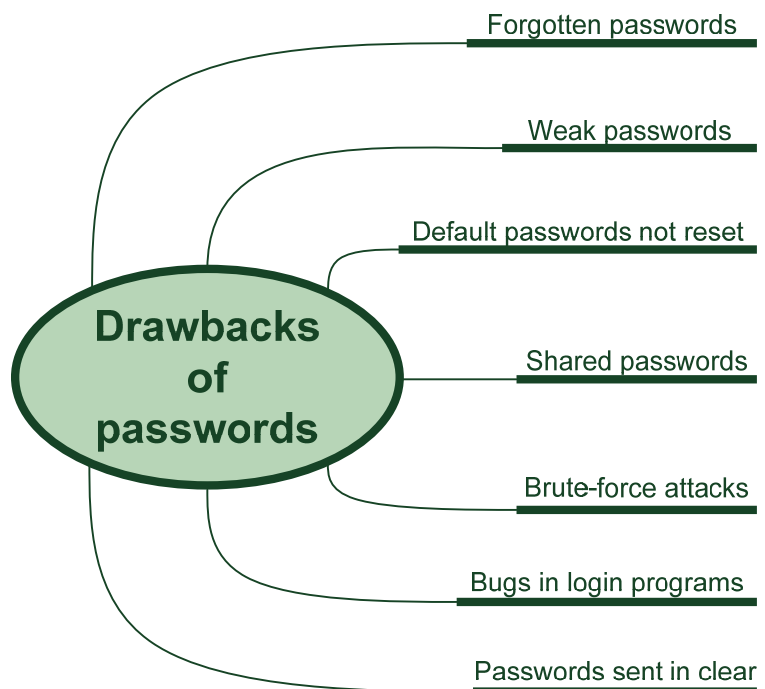
Summary

This technical briefing paper outlines multifactor authentication methods that supplement the traditional passwords and PIN codes with security tokens, digital certificates and biometrics.

Introduction

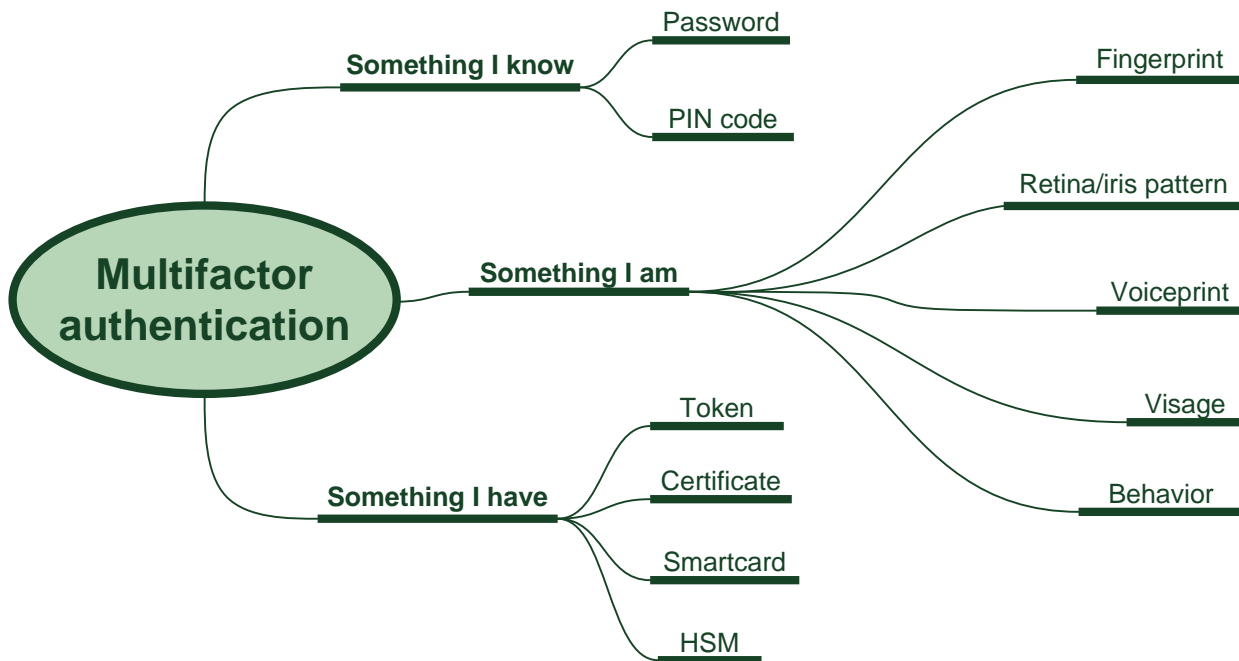
We are all familiar with single-factor authentication in the form of the conventional system or network login process. It's simple to enter a username and password but the process is vulnerable to certain problems:

- Users sometimes forget their passwords, requiring mechanisms for them to re-authenticate themselves before being issued with replacement passwords;
- Users typically choose relatively weak passwords that are easy to guess, unless password length, complexity and re-use rules are applied which, in turn, make passwords harder to remember;
- Default passwords are often well-known. Passwords that are reset to weak choices by 'helpful' IT Support Desks are also liable to be guessed;
- Passwords are supposed to be kept secret but can be shared very easily in practice;
- Passwords on many systems can be broken by brute-force attacks, trying all possible combinations of characters. Long passwords make this attack more difficult but, again, long passwords are more likely to be forgotten;
- Bugs and implementation or configuration problems occasionally surface in login programs and the associated processes, such that hackers may be able to bypass logins altogether. Anonymous and guest user logins, for example, are convenient in some cases but may open the door to unauthorized access. WEP and WPA protocols for authenticating Wi-Fi users have both been broken by wireless hackers;
- Passwords can sometimes be captured 'in the clear' (*i.e.* before the point that they are encrypted or hashed by the system). Aging network protocols such as FTP and POP3 don't help by passing unencrypted passwords over the network.



In short, we need better, more secure methods of authenticating users than passwords in many cases.

Multifactor authentication



'Multifactor' refers to combining two or more of the following three categories*:

1. **Something you know** e.g. a password, passphrase or PIN code;
2. **Something you have** e.g. a security token, private key *etc.*;
3. **Something you are** e.g. a biometric feature such as a fingerprint, iris or retina pattern.

Note that two or more items from one category count as one factor. It doesn't matter how many passwords you demand from me, they are all "something I know" and are all vulnerable to the same problems as noted above. Having discussed passwords, we turn now to other authentication methods.

Security tokens

In the physical world, a key to a lock is a security token. Without the key, I cannot (easily) open the lock. Electronic equivalents of keys for the online world include:

- Tokens are electronic devices such as proximity cards that are often used to control access to computer rooms *etc.* and are sometimes used for user authentication to computers, especially in situations where users have to be mobile and logon/logoff time is critical (e.g. medical staff accessing systems in an emergency ward). Cryptographic tokens such as SecureID use cryptographic algorithms to create sequences of apparently random but in fact predictable outputs. Software on the authentication servers synchronize their cryptographic algorithms with the tokens and so can calculate what each token should be displaying at any point in time. Security tokens are becoming available with built-in keypads for users to enter PIN codes to enable the display and, potentially, for users to enter transaction data for signing;
- Digital certificates containing public keys corresponding to private keys known only to the system or user. Private keys can be used to encrypt and "sign" messages digitally, and the signatures can be verified by decrypting them using the public keys held on the certificates. Forged signatures or altered messages should be detected when they are verified;

* Some would add a fourth category: 'something you do' *i.e.* behavioral characteristics such as typing rates *etc.* although these could also be categorized as biometrics.

- Smart cards may be used to store digital certificates, cryptographic keys *etc.* Secure smart cards are engineered such that secrets are never disclosed outside the card itself, with the cryptographic processing being performed on the card. Anti-tamper controls prevent the secrets being revealed by physical compromise of the card to investigate the embedded chip;
- Hardware [or High] Security Modules are essentially big secure cryptographic smart cards with more powerful processors and larger storage. They are physically hardened and, again, have anti-tamper controls. They are used in some military and financial services applications where the impacts of keys being compromised justify the expense.

Just as in the physical world, the strength of security tokens and indeed other authenticators depends partly on the quality of the implementation. Badly designed or worn locks can be picked more easily than “high security” locks that are properly maintained. Badly designed or mis-configured authentication systems may be bypassed or broken by hackers.

Biometrics

Biometrics are characteristic biological features that allow us to differentiate individuals. Examples:

- Fingerprints and palm prints can be measured by various types of scanner. Simple types may be fooled by latex copies whereas more sophisticated ones incorporate additional features such as temperature and/or blood flow sensors to disregard crude forgeries;
- Retinal scanners scan the pattern of blood vessels in the retinal layer inside the rear of our eyeballs using a low power laser. The pattern varies between individuals due to a combination of their genetics and chance events as the eyes developed. A warning sign seen in many optical science labs suggests why retinal scanners are generally unpopular: “Do not stare at laser with remaining eye”;
- Iris scanners are similar to retinal scanners but scan the colored front part of the eye, which is also highly variable between individuals. This is considered less invasive than retinal scans, especially if low-level plain or infra red light is used instead of lasers;
- Voice prints measure distinctive characteristics of a person’s speaking voice. Restricted bandwidth makes telephone voice prints somewhat less reliable than using high quality audio directly from a decent microphone, but some banks have been trialing voice-print customer authentication for telephone banking and support purposes;
- Visage or facial recognition systems use characteristics such as nose length, distance between the eyes, thermal patterns *etc.* to map a person’s face and compare this to representations stored at an earlier registration step using pattern recognition techniques. Characteristics such as hand geometry, vein patterns, body shape and even gait have been used from time to time in laboratory experiments but seldom make it into full commercial use;
- Behavioral traits such as the natural rhythm of a person’s typing or the normal sequence in which they access applications and functions *etc.* can help build a computer’s-eye picture of the person behind the keyboard;
- The angles, speeds/rates of change and pressures applied when a person signs their name on a pressure-sensitive tablet can all be measured and used as authenticators;
- DNA fingerprinting is an extremely accurate method of identifying individuals with tremendous applications in forensic science. It is far too slow for routine authentication (imagine having to wait a week or more to login!) but could potentially be used as an ultimate reference method for the victims of identity theft to confirm their true identities, provided reliable reference samples had been taken earlier and stored securely, and provided proper scientific tests and sample handling techniques were followed rigorously – significant assumptions in themselves.

All practical biometric systems require initial registration of individuals plus occasional re-registration to account for the normal human aging process – and, yes, this represents a common weak point. If I am able to dupe the system into accepting my biometrics under your name, then the system will henceforth believe that I am you.

All biometric systems also suffer the problems caused by natural biological variations in an individual's characteristics (e.g. my voiceprint may change substantially if I have a cold, and may not be available at all if I suffer laryngitis), and in the presentation/measurement of a person's features (e.g. the volume level or the words that I speak may vary). In practice this means that they all have to allow a margin of error and this of course increases the possibility of mistakes. Setting the error level is a balance between having too many false negatives (genuine individuals who are rejected by the system) and too many false positives (imposters who are accepted). The margin of error can be reduced by better quality biometric systems or by taking more measurements, perhaps combining results from several sources.

The following table from "The '123' of Biometric Technology" by Yau Wei Yun compares common biometric methods (see [Wikipedia](#) for an explanation of the terms used):

Biometrics	Univer- sality	Unique- ness	Perma- nence	Collect- ability	Perfor- mance	Accept- ability	Circum- vention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

H=High, M=Medium, L=Low

Conclusion

Two-factor authentication ("2FA") is an emerging best practice for authentication of remote users such as online banking customers and roaming employees who need access to the corporate network from untrusted systems and locations. As multifactor authentication enters the mainstream and prices fall, it is gradually becoming economic for authentication of local users as well, particularly for privileged users and for access to important systems, functions or transactions. Think about it: would you be confident if password was all that was needed to launch a missile?

For more information

For general advice on information security controls including those identified in this briefing, contact the Information Security Manager, visit Information Security Management's intranet website or browse the NoticeBored links collections on [identity theft](#) and [authentication](#). The [Wikipedia entry for biometrics](#) is particularly helpful and has a good selection of references.